EXHIBIT A

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

DIVISION OF BANKING
SUPERVISION AND REGULATION

DIVISION OF CONSUMER
AND COMMUNITY AFFAIRS

SR 08-8 / CA 08-11

October 16, 2008

TO THE OFFICER IN CHARGE OF SUPERVISION AND APPROPRIATE SUPERVISORY AND EXAMINATION STAFF AT EACH FEDERAL RESERVE BANK AND CERTAIN ORGANIZATIONS SUPERVISED BY THE FEDERAL RESERVE

SUBJECT: **Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles**

In recent years, banking organizations have greatly expanded the scope, complexity, and global nature of their business activities. At the same time, compliance requirements associated with these activities have become more complex. As a result, organizations have confronted significant risk management and corporate governance challenges, particularly with respect to compliance risks that transcend business lines, legal entities, and jurisdictions of operation.[1] To address these challenges, many banking organizations have implemented or enhanced firmwide compliance risk management programs and program oversight.

While the guiding principles of sound risk management are the same for compliance as for other types of risk, the management and oversight of compliance risk presents certain challenges. For example, quantitative limits reflecting the board of directors' risk appetite can be established for market and credit risks, allocated to the various business lines within the organization, and monitored by units independent of the business line. Compliance risk does not lend itself to similar processes for establishing and allocating overall risk tolerance, in part because organizations must comply with applicable rules and standards. Additionally, existing compliance risk metrics are often less

meaningful in terms of aggregation and trend analysis as compared with more traditional market and credit risk metrics. These distinguishing characteristics of compliance risk underscore the need for a firmwide approach to compliance risk management and oversight for large, complex organizations. A firmwide compliance function that plays a key role in managing and overseeing compliance risk while promoting a strong culture of compliance across the organization is particularly important for large, complex organizations that have a number of separate business lines and legal entities that must comply with a wide range of applicable rules and standards.

The Federal Reserve has, primarily through the examination process, emphasized the need for effective firmwide compliance risk management and oversight at large, complex banking organizations. While firmwide compliance risk management programs and oversight at the largest supervised banking organizations have generally improved, the level of progress at individual banking organizations varies and opportunity for improvement remains. The Federal Reserve strongly encourages large banking organizations with complex compliance profiles to ensure that the necessary resources are dedicated to fully implementing effective firmwide compliance risk management programs and oversight in a timely manner.[2]

The Federal Reserve's expectations for all supervised banking organizations are consistent with the principles outlined in a paper issued in April 2005 by the Basel Committee on Banking Supervision, entitled *Compliance and the compliance function in banks* (Basel compliance paper). The principles in the Basel compliance paper have become widely recognized as global sound practices for compliance risk management and oversight, and the Federal Reserve endorses these principles. Nevertheless, some banking organizations have sought clarification as to the Federal Reserve's views regarding certain compliance risk management and oversight matters. This SR/CA letter clarifies Federal Reserve views applicable to large banking organizations with complex compliance profiles in the following areas where guidance has been requested:

I. Organizations that should implement a firmwide approach to compliance risk management and oversight;
II. Independence of compliance staff;
III. Compliance monitoring and testing; and
IV. Responsibilities of boards of directors and senior management regarding compliance risk management and oversight.

I. Firmwide Compliance Risk Management and Oversight

Overview

Organizations supervised by the Federal Reserve, regardless of size and complexity, should have effective compliance risk management programs that are appropriately tailored to the organizations' risk profiles.[3] The manner in which the program is implemented and the type of oversight needed for that program can vary considerably depending upon the scope and complexity of the organization's activities, the geographic reach of the organization, and other inherent risk factors. Larger, more complex banking organizations tend to conduct a wide range of business activities that are subject to complex compliance requirements that frequently transcend business lines and legal entities and, accordingly, present risk management and corporate governance challenges. Consequently, these organizations typically require a firmwide approach to compliance risk management and oversight that includes a corporate compliance function. In contrast, smaller, less-complex banking organizations are not generally confronted with the types of compliance risks and challenges that require a comprehensive firmwide approach to effectively manage and oversee compliance risk. The following discussion, therefore, is *not* directed at smaller, less-complex banking organizations.

Firmwide compliance risk management refers to the processes established to manage compliance risk across an entire organization, both within and across business lines, support units, legal entities, and jurisdictions of operation. This approach ensures that compliance risk management is conducted in a context broader than would take place solely within individual business lines or legal entities. The need for a firmwide approach to compliance risk management at larger, more complex banking organizations is well demonstrated in areas such as anti-money laundering, privacy, affiliate transactions, conflicts of interest, and fair lending, where legal and regulatory requirements may apply to multiple business lines or legal entities within the banking organization. Certain other compliance risks may also warrant a firmwide risk management approach to address similar rules and standards that apply to the organization's operations across different jurisdictions. In all such instances, compliance risk management benefits from an aggregate view of the organization's compliance risk exposure and an integrated approach to managing those risks.

The processes established for managing compliance risk on a firmwide basis should be formalized in a compliance *program* that establishes the framework for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risks across the organization, and for providing compliance training throughout the organization. A banking organization's compliance risk

management program should be documented in the form of compliance policies and procedures and compliance risk management standards.[4]

Firmwide compliance oversight refers to the processes established to oversee compliance risk management across the entire organization, both within and across business lines, legal entities, and jurisdictions of operation. In addition to the oversight provided by the board of directors and various executive and management committees of an organization, a key component of firmwide compliance oversight in larger, more complex banking organizations is a corporate compliance function that has day-to-day responsibility for overseeing and supporting the implementation of the organization's firmwide compliance risk management program, and that plays a key role in controlling compliance risks that transcend business lines, legal entities, and jurisdictions of operation.

Federal Reserve Supervisory Policies

Large Banking Organizations with Complex Compliance Profiles. Although balance sheet size is not the defining indication of a banking organization's compliance risk management needs, experience has demonstrated that banking organizations with $50 billion or more in consolidated total assets typically have multiple legal entities that pose the type of compliance risks and challenges that call for a comprehensive firmwide approach to appropriately control compliance risk and provide effective oversight. Accordingly, such organizations should generally implement firmwide compliance risk management programs and have a corporate compliance function.

Compliance programs at such organizations should include more robust processes for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk, and for providing compliance training throughout the organization in order to appropriately control the heightened level and complexity of compliance risk. The corporate compliance function should play a key role in overseeing and supporting the implementation of the compliance risk management program, and in controlling compliance risks that transcend business lines, legal entities, and jurisdictions of operation.[5]

Large Banking Organizations with Less-Complex Compliance Profiles. In some instances, banking organizations that meet the $50 billion asset threshold may have few legal entities, be less complex in nature, and may engage in only a very limited range of business activities. Such organizations may be able to effectively manage and oversee compliance risk without implementing a comprehensive firmwide approach. Alternatively, these organizations may choose to implement a

firmwide approach whose scope is highly risk-focused on particular compliance risks that exist throughout the organization. In lieu of relying on a corporate compliance function to play a key role in providing day-to-day oversight of the compliance program, these organizations may rely on executive and management committees that are actively involved in providing ongoing corporate oversight of the compliance risk management program. An organization that adopts this approach, however, should ensure that its compliance program incorporates controls that effectively address compliance risks that transcend business lines, legal entities, and jurisdictions of operation; that appropriate firmwide standards are established for the business lines to follow in managing compliance risk and reporting on key compliance matters; and that the organization is appropriately overseeing the implementation of its compliance risk management program.

Foreign Banking Organizations. Each foreign banking organization supervised by the Federal Reserve should implement a compliance program that is appropriately tailored to the scope, complexity, and risk profile of the organization's U.S. operations. The program should be reasonably designed to ensure that the organization's U.S. operations comply with applicable U.S. rules and standards, and should establish effective controls over compliance risks that transcend business lines or legal entities. Foreign banking organizations with large, complex U.S. operations should implement compliance programs for these operations that have more robust processes for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk, and for providing compliance training, than would be appropriate for foreign banking organizations with smaller, less-complex U.S. operations.[6]

With respect to oversight, foreign banking organizations should provide effective oversight of compliance risks within their U.S. operations, including risks that transcend business lines or legal entities. A foreign banking organization, however, has flexibility in organizing its oversight structure. Compliance oversight of U.S. activities may be conducted in a manner that is consistent with the foreign banking organization's broader compliance risk management framework. Alternatively, a separate function may be established specifically to provide compliance oversight of the organization's U.S. operations. Regardless of the oversight structure utilized by a foreign banking organization, its established oversight mechanisms, governing policies and procedures, and supporting infrastructure for its U.S. operations should be sufficiently transparent for the Federal Reserve to assess their adequacy.

II. Independence of Compliance Staff

Federal Reserve supervisory findings at large, complex banking organizations consistently reinforce the need for compliance staff to be appropriately independent of the business lines for which they have compliance responsibilities. Compliance independence facilitates objectivity and avoids inherent conflicts of interest that may hinder the effective implementation of a compliance program. The Federal Reserve has observed compliance independence to be an area in which there is considerable variation in practices, some of which do not consistently meet supervisory standards. A particular challenge for many organizations is attaining an appropriate level of independence with respect to compliance staff operating within the business lines.

The Federal Reserve does not prescribe a particular organizational structure for the compliance function. Large banking organizations with complex compliance profiles are encouraged, however, to avoid inherent conflicts of interest by ensuring that accountability exists between the corporate compliance function and compliance staff within the business lines. Such accountability would provide the corporate compliance function with ultimate authority regarding the handling of compliance matters and personnel decisions and actions relating to compliance staff, including retaining control over the budget for, and remuneration of, all compliance staff.[7] Compliance independence should not, however, preclude compliance staff from working closely with the management and staff of the various business lines. To the contrary, compliance functions are generally more effective when strong working relationships between compliance and business line staff exist.

The Federal Reserve recognizes, however, that many large, complex banking organizations have chosen to implement an organizational structure in which compliance staff within a business line have a reporting line into the management of the business. In these circumstances, compliance staff should also have a reporting line through to the corporate compliance function with respect to compliance responsibilities. In addition, a banking organization that chooses to implement such a dual reporting structure should ensure that the following minimum standards are observed in order to minimize potential conflicts of interest associated with this approach:

(1) In organizations with dual reporting line structures, the corporate compliance function should play a key role in determining how compliance matters are handled and in personnel decisions and actions (including remuneration) affecting business line compliance and local compliance staff, particularly senior compliance staff. Furthermore, the organization should have in place a process designed to ensure that disputes between the corporate compliance function and

business line management regarding compliance matters are resolved objectively. Under such a process, the final decision-making authority should rest either with the corporate compliance function, or with a member or committee of senior management that has no business line responsibilities.

(2) Compensation and incentive programs should be carefully structured to avoid undermining the independence of compliance staff. Compliance staff should not be compensated on the basis of the financial performance of the business line. Such an arrangement creates an improper conflict of interest.

(3) Banking organizations with dual reporting line structures should implement appropriate controls and enhanced corporate oversight to identify and address issues that may arise from conflicts of interest affecting compliance staff within the business lines. For example, in these circumstances, the process for providing corporate oversight of monitoring and testing activities performed by compliance staff within the business lines should be especially robust.

III. Compliance Monitoring and Testing

Robust compliance monitoring and testing play a key role in identifying weaknesses in existing compliance risk management controls and are, therefore, critical components of an effective firmwide compliance risk management program. Federal Reserve supervisory findings at large, complex banking organizations indicate that opportunities for improving compliance monitoring and testing programs at many of these organizations remain.

Risk Assessments and Monitoring and Testing Programs. Risk assessments are the foundation of an effective compliance monitoring and testing program. The scope and frequency of compliance monitoring and testing activities should be a function of a comprehensive assessment of the overall compliance risk associated with a particular business activity.[8] Many larger, more complex banking organizations, however, remain in the process of implementing comprehensive risk assessment methodologies. This presents a challenge to the effectiveness of compliance monitoring and testing programs as the effectiveness of these programs relies upon comprehensive risk assessments. Larger, more complex banking organizations are strongly encouraged to complete the implementation of comprehensive risk assessment methodologies and to ensure that compliance monitoring and testing activities are based upon the resulting risk assessments.

Testing. Although the Federal Reserve has generally observed considerable progress in the level of compliance monitoring, there continues to be room for

improvement regarding the testing of compliance controls. Compliance testing is necessary to validate that key assumptions, data sources, and procedures utilized in measuring and monitoring compliance risk can be relied upon on an ongoing basis and, in the case of transaction testing, that controls are working as intended. The testing of controls and remediation of deficiencies identified as a result of testing activities are essential to maintaining an effective internal control framework.

The scope and frequency of compliance testing activities should be based upon the assessment of the specific compliance risks associated with a particular business activity. Periodic testing of compliance controls by compliance staff is strongly encouraged as this practice tends to result in an enhanced level of compliance testing. If, however, compliance testing is performed exclusively by the internal audit function, particular care should be taken to ensure that high-risk compliance elements are not otherwise obscured by a lower overall risk rating of a broadly defined audit entity. Otherwise, the scope and frequency of audit coverage of higher-risk compliance elements tends to be insufficient.

IV. Responsibilities of the Board of Directors and Senior Management

The primary responsibility for complying with applicable rules and standards rests with the individuals within the organization as they conduct their day-to-day business and support activities. The board, senior management, and the corporate compliance function are responsible for working together to establish and implement a comprehensive and effective compliance risk management program and oversight framework that is reasonably designed to prevent and detect compliance breaches and issues.

Boards of Directors.[9] Boards of directors are responsible for setting an appropriate culture of compliance within their organizations, for establishing clear policies regarding the management of key risks, and for ensuring that these policies are adhered to in practice. The following discussion is intended to clarify existing Federal Reserve supervisory views with regard to responsibilities of the board related to compliance risk management and oversight, and to differentiate these responsibilities from those of senior management.

To achieve its objectives, a sound and effective firmwide compliance risk management program should have the support of the board and senior management. As set forth in applicable law and supervisory guidance, the board and senior management of a banking organization have different, but

complementary, roles in managing and overseeing compliance risk.[10]

The board has the responsibility for promoting a culture that encourages ethical conduct and compliance with applicable rules and standards. A strong compliance culture reinforces the principle that an organization must conduct its activities in accordance with applicable rules and standards, and encourages employees to conduct all activities in accordance with both the letter and the spirit of applicable rules and standards. The board should have an appropriate understanding of the types of compliance risks to which the organization is exposed. The level of technical knowledge required of directors to fulfill these responsibilities may vary depending on the particular circumstances at the organization.

The board should ensure that senior management is fully capable, qualified, and properly motivated to manage the compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations. The board should ensure that its views about the importance of compliance are understood and communicated by senior management across, and at all levels of, the organization through ongoing training and other means. The board should ensure that senior management has established appropriate incentives to integrate compliance objectives into the management goals and compensation structure across the organization, and that appropriate disciplinary actions and other measures are taken when serious compliance failures are identified. Finally, the board should ensure that the corporate compliance function has an appropriately prominent status within the organization. Senior management within the corporate compliance function and senior compliance personnel within individual business lines should have the appropriate authority, independence, and access to personnel and information within the organization, and appropriate resources to conduct their activities effectively.

The board should be knowledgeable about the general content of the compliance program and exercise appropriate oversight of the program. Accordingly, the board should review and approve key elements of the organization's compliance risk management program and oversight framework, including firmwide compliance policies, compliance risk management standards, and roles and responsibilities of committees and functions with compliance oversight responsibilities. The board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by senior management. The board should exercise reasonable due diligence to ensure that the compliance program remains effective by at least annually reviewing a report on the effectiveness of the program. The board may delegate

these tasks to an appropriate board-level committee.

Senior Management. Senior management across the organization is responsible for communicating and reinforcing the compliance culture established by the board, and for implementing measures to promote the culture. Senior management also should implement and enforce the compliance policies and compliance risk management standards that have been approved by the board. Senior management of the corporate compliance function should establish, support, and oversee the organization's compliance risk management program. The corporate compliance function should report to the board, or a committee thereof, on significant compliance matters and the effectiveness of the compliance risk management program.

Senior management of a foreign banking organization's U.S. operations should provide sufficient information to governance or control functions in its home country, and should ensure that responsible senior management, including in the home country, maintain a thorough understanding of the risk and control environment governing U.S. operations. U.S. management should assess the effectiveness of established governance and control mechanisms on an ongoing basis, including processes for reporting and escalating areas of concern and implementation of corrective action as necessary.

V. Conclusion

This SR/CA letter should be disseminated to all large, complex banking organizations, and other institutions supervised by the Federal Reserve as Reserve Bank staff believes appropriate. Questions may be directed to Karen El Kochta, Senior Supervisory Financial Analyst, Compliance Risk, Division of Banking Supervision and Regulation, at (202) 452-5206; Chris Laursen, Manager, Risk Policy & Guidance, Division of Banking Supervision and Regulation, at (202) 452-2478; or Phyllis Harwell, Manager, Division of Consumer and Community Affairs, at (202) 452-3658. In addition, questions may be sent via the Board's public website.[11]

signed by
Deborah P. Bailey
Deputy Director
Division of Banking
Supervision and Regulation

signed by

Glenn E. Loney
Deputy Director
Division of Consumer
and Community Affairs

Cross Reference:

SR letter 04-18, "Bank Holding Company Rating System"

SR letter 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies"

Notes:

1. Compliance risk is the risk of legal or regulatory sanctions, financial loss, or damage to reputation resulting from failure to comply with laws, regulations, rules, other regulatory requirements, or codes of conduct and other standards of self-regulatory organizations applicable to the banking organization (applicable rules and standards). (See, generally, *Compliance and the compliance function in banks*, Basel Committee on Banking Supervision, April 2005, www.bis.org.) Return to text

2. Effective compliance risk management programs incorporate controls designed to maintain compliance with applicable rules and standards, including safety and soundness and consumer protection guidance issued by supervisory authorities. Return to text

3. See SR letter 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies." This letter provides general guidance on risk management processes and internal controls for consolidated organizations, and discusses the elements of a sound risk management system applicable to all banking organizations for which the Federal Reserve has supervisory responsibility. SR 95-51 states that all bank holding companies should be able to assess the major risks of the consolidated organization. See also 12 CFR Part 208, appendix D-1, "Interagency Guidelines Establishing Standards for Safety and Soundness." Return to text

4. *Compliance policies* refer to both: (1) firmwide compliance policies that apply to all employees throughout the organization as they conduct their business and support activities; and (2) the more detailed, business-specific

policies that are further tailored to, and more specifically address, compliance risks inherent in specific business lines and jurisdictions of operation, and apply to employees conducting business and support activities for the specific business line and/or jurisdiction of operation. *Compliance procedures* refer to the control procedures that are designed to implement compliance policies. *Compliance risk management standards* refer to policies and procedures applicable to compliance staff as they fulfill their day-to-day compliance responsibilities. Compliance standards should clearly articulate expectations regarding the processes to be followed in implementing the organization's firmwide compliance risk management program, including the processes and criteria to be utilized in identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk, and in providing compliance training. Compliance standards should also clearly articulate the roles and responsibilities of the various committees, functions, and staff with compliance support and oversight responsibilities. Return to text

5. While the corporate compliance function is generally responsible for overseeing and supporting the compliance risk management program, it is recognized that the board of directors may assign primary responsibility for aspects of the compliance program to other units within the organization (e.g., finance, information technology, human resources, etc.). The corporate compliance function, therefore, may or may not have responsibility for monitoring and testing the controls over certain compliance activities embedded within these units, such as those over regulatory reporting and regulatory capital. Nevertheless, it is important that an organization's compliance program incorporates appropriate controls over these risks and that proper oversight of the management of these risks is conducted. Return to text

6. Foreign banking organizations with $50 billion or more in U.S. third-party assets will generally be considered as large banking organizations with complex compliance profiles for purposes of this SR/CA letter unless their U.S. activities are less complex in nature as described in Section I of this letter. The Federal Reserve's views on compliance risk management programs apply equally to the large, complex U.S. operations of foreign banking organizations. Return to text

7. The reference to all compliance staff includes corporate, business line, and local compliance staff. Return to text

8. Risk assessments should be based upon firmwide standards which establish the method for, and criteria to be utilized in, assessing risk throughout the

organization. Risk assessments should take into consideration both the risk inherent in the activity, and the strength and effectiveness of controls designed to mitigate the risk. Return to text

9. Foreign banking organizations should ensure that, with respect to their U.S. operations, the responsibilities of the board described in this section are fulfilled in an appropriate manner through their oversight structure and risk management framework. Return to text

10. See, for example, the Basel compliance paper; SR letter 04-18, "Bank Holding Company Rating System"; SR letter 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies"; and the United States Sentencing Commission's *Federal Sentencing Guidelines Manual*, Chapter Eight, "Sentencing of Organizations." Return to text

11. See http://www.federalreserve.gov/feedback.cfm Return to text